North Dakota Homeland Security Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

North Dakota has first confirmed anthrax case of the year. North Dakota's state veterinarian is urging ranchers to protect their animals against anthrax. She said an anthrax case has been confirmed in eastern Sioux County - the first in that area in many years. It also is the first confirmed case in the state this year. The state veterinarian is urging ranchers to make sure their animals are properly vaccinated. Anthrax bacteria spores lie dormant in the ground and become active under conditions such as heavy rainfall, flooding or drought. North Dakota usually has a few anthrax cases every year. In 2005, the disease resulted in an estimated 1,000 dead cattle, bison, horses, sheep, llamas and farmed deer and elk. Source: http://www.bovinevetonline.com/newsCN.asp?contentid=1082361

ND refinery ending month-long maintenance. A month-long $125-million overhaul at Tesoro Corp.'s Mandan, North Dakota refinery will be completed on time and within budget, the company said. North Dakota's sole oil refinery was idled April 16 for maintenance and upgrades. The work included installation of additional pollution controls, and bumping up the capacity by about 2,000 barrels daily of ultra-low sulfur diesel fuel used in off-road construction and farm equipment. Work is slated to be finished this week with start-up scheduled for early next week. Production in North Dakota's prolific oil patch continues to grow exponentially, with a record number of wells drawing crude at nearly twice the daily rate of two years ago. At the current pace, North Dakota is quickly gaining ground on California, the nation's third-biggest oil producer, industry officials say. Source: http://www.thesunnews.com/2010/05/19/1483543/nd-refinery-ending-monthlong-maintenance.html

Regional

(Minnesota) **Twin Cities nurses authorize strike.** Nurses working at Twin Cities hospitals voted Wednesday night to authorize a strike. More than 90 percent of the 9,000 nurses voting rejected labor contracts proposed by local hospitals. At least 60 percent needed to reject the contracts if union leadership was to have the authority to call a strike. The Minnesota Nurses Association said in a press statement it will submit a 10-day strike notice to hospitals in coming days. After a one-day strike, nurses will turn in a formal request to go back to work. The association claims the strike would be the largest in U.S. history. Source: http://www.bizjournals.com/twincities/stories/2010/05/17/daily32.html

(Montana) **Bank phone scam targets locals.** Montanans are being targeted by a new version of a phone scam, the Montana attorney general warned May 17. A Libby resident reported to authorities that she had received a phone call purportedly from First National Bank requesting her ATM card information. She did what bank and law-enforcement officials advise — refused to give out sensitive personal or financial information. She hung up and reportedly contacted First Montana Bank (formally First National Bank) and learned that several customers have received the same phone call scam. The attorney general's Office of Consumer Protection became aware of the scam when its lead

attorney also received an automated call on his cell phone claiming to be from First National Bank. The message said his ATM card had been "suspended because it was compromised" and directed him to press 1 and then to enter his 14-digit ATM card number. The lead attorney hung up without providing the information and instead called the bank. The chief executive officer with First Montana Bank confirmed that the phone pitch is a scam and that he has heard from half a dozen customers who have provided their card numbers. While the message purports to be from First National Bank, the calls are part of a "phishing" scam that tries to trick unsuspecting consumers into giving up their personal account information. Source: http://www.thewesternnews.com/news/article_505bee22-6453-11df-8c26-001cc4c002e0.html

(South Dakota) **Sioux Falls neighborhood evacuated for gas issue.** The smell of gas in a Sioux Falls, South Dakota neighborhood forced several residents out of their homes for a few hours. The odor was reported just before 6 p.m. May 14. The Sioux Falls fire department said a MidAmerican Energy worker found natural gas readings from a house that had been vacant for some time and shut off gas to the building. Power to the neighborhood was shut off until fire crews could ventilate the house. As a precaution, nearby residents were evacuated. They were allowed to return about 8:15 p.m. No injuries were reported Source: http://www.ktiv.com/Global/story.asp?S=12487323

National

Immigration groups escalate tactics. Immigrant-rights groups say they are stepping up their tactics to prompt action from Congress on immigration. They are planning to block buses leaving deportation centers, stage sit-ins in lawmakers' offices, and protest companies doing business in Arizona. Those actions in Seattle, Los Angeles, New York and Washington, D.C. will culminate May 29, when groups from across the nation will gather in Arizona for a protest. Many of those protest actions could result in arrests. Students were arrested in Arizona Monday while protesting at an Arizona Senator's office and are expected to face deportation hearings. "Many more will step forward to put their bodies on the line in the weeks to come," an official with the Center for Community Change said on a conference call with reporters Tuesday. He emphasized that none of the planned activities will be violent. The May 29 protest coincides with events being planned by conservative and tea party groups. Source: http://www.congress.org/news/2010/05/18/immigration_groups_escalate_tactics

(California) **Navy enlists sea mammals to defend California ports.** The U.S. Navy is showing off some unlikely recruits in California. Its Marine Mammal Program conducted training exercises Tuesday in the San Francisco Bay using sea lions and dolphins that have been trained to perform underwater surveillance for object detection, location, marking, and recovery. In a full-scale regional exercise focusing on the state's response and recovery to multiple terrorist attacks at Bay Area ports, federal, state, and city officials took part in the Golden Guardian emergency preparedness program. At Pier 48 in San Francisco, the city's police and fire departments, along with its Emergency Operations Center, conducted a drill demonstrating the ability of dolphins and California sea lions to help protect coastal areas from maritime attacks. Source: http://news.cnet.com/2300-11386_3-10003492.html?tag=mncol

(New York) **After copier fiasco, FTC may regulate.** It was a startling wake-up call for anyone using a digital copier. A CBS News investigation found confidential Buffalo, New York Police records in a copier sent to New Jersey. New federal regulations may follow. Four weeks after CBS News bought a

few used digital copiers and found sensitive Buffalo Police information still on them, a Massachusetts Congressman is calling for an investigation by the Federal Trade Commission. He said, "We have to do a lot more to ensure the public and corporations know this, and that absolute security is applied to copy machines across our country." The FTC has already responded, saying it shares the Representative's concern, and that it has begun reaching out to copier manufacturers and resellers to ensure that they are aware of the privacy risks and are warning customers of those risks. The city of Buffalo found out the hard way in January after trading in two old digital copiers from Buffalo Police Headquarters that ended up in a warehouse in New Jersey. CBS bought them for $300 apiece and on the hard drive were still lists of domestic violence complaints and targets of a major drug raid. On the same day, CBS bought an old copier that had been used by a health insurance company that still had confidential medical records on it. Source: http://www.wivb.com/dpp/news/local/After-copier-fiasco-FTC-may-regulate

Taiwan man pleads guilty in Iran missile case. A Taiwanese businessman pleaded guilty May 13 to federal charges arising from an undercover investigation into the illegal export to Iran of items that can be used for missiles, unmanned drones, and other military purposes. He pleaded guilty to conspiring to violate the U.S. embargo against Iran and attempting to export prohibited goods that have dual civilian and military uses. The citizen of Taiwan also entered guilty pleas on behalf of his Landstar Tech Co. He was arrested in February in Guam in the midst of a transaction to ship to Iran some 8,500 glass-to-metal seals and 120 military-grade connectors. Commerce Department investigators said the suspect had arranged at least 30 banned shipments to Iran since 2007, falsely telling U.S.-based suppliers in Lakewood, New Jersey, Cincinnati, and elsewhere that the goods were destined for Hong Kong or Taiwan. The e-mails show he shipped two P200 Turbine engines and spare parts to Iran via Hong Kong in 2007, labeling them on an invoice as "a starter for a car and wheels." The engines can be used in model aircraft but also for military drones. Source: http://www.google.com/hostednews/ap/article/ALeqM5gZ717fMuW51yLZIHWmgXUFOcDbLAD9FM1SS80

INTERNATIONAL

NATO should tool up for cyber war, say globo-bigwigs. The North Atlantic Treaty Organization (NATO) believes there is not likely to be a conventional military attack on its members in the future, but that some form of cyber-attack is one of three most probable dangers facing the alliance. The organization is the midst of finding itself a new purpose. A group of bigwigs have been appointed to find "a New Strategic Concept". NATO has gone through several changes since its creation in the wake of the Second World War as a defensive alliance against the Soviet Union. Although NATO said the possibility of conventional military attack could not be ignored, it is more likely to face an attack by ballistic missile, a terrorist attack or a cyber attack. Dealing with cyber attacks will require more cooperation with the European Union, the experts conclude, because the EU has more expertise in dealing with such attacks. The report warns: "The next significant attack on the Alliance may well come down a fiber optic cable. Already, cyber attacks against NATO systems occur frequently, but most often below the threshold of political concern." It recommends a major effort to increase monitoring of NATO's critical network in order to find and fix vulnerabilities. The Civil- Military Cooperation Centre for Excellence should improve members' training in cyber-defense. NATO members should expand their early-warning, network-monitoring systems. NATO should have a team ready to dispatch to areas under or threatened by cyber attack. Finally the experts said that over

time, NATO should "plan to mount a fully adequate array of cyber-defense capabilities, including passive and active elements." Source: http://www.theregister.co.uk/2010/05/18/nato_cyber_defence/

Canada warns of second measles outbreak. Five confirmed cases of measles in Alberta, Canada, have led to officials with Alberta Health Services requesting residents to get measles vaccines, according to iNews880.com. The five confirmed cases all occurred within the past week. Officials said the first confirmed case was a toddler a week ago. On May 14, Alberta Health Services officials reported there were four new confirmed cases. Even though the strain seems to be the same as a recent outbreak in British Columbia, the two outbreaks do not appear to be connected. More than two dozen people contracted the illness in British Columbia in April, according to assorted wire reports. Source: http://vaccinenewsdaily.com/news/213068-canada-warns-of-second-measles-outbreak

Iraq football stadium hit by deadly suicide bombing. A suicide bombing at a football stadium in northern Iraq has killed 10 people and injured 120 others. An attacker detonated explosives hidden inside a vehicle at the entrance to the stadium in Tal Afar, a mainly Shia Turkmen town west of Mosul. Witnesses said the blast was followed by at least one other. Some of them said up to three suicide bombers were involved. No group has yet said it carried out the bombings in Tal Afar, but correspondents said the method was similar to past al-Qaeda attacks and the group remains active in the area. Source: http://news.bbc.co.uk/2/hi/middle_east/8683642.stm

Al Qaeda in Iraq was planning attack on World Cup. A senior member of Al Qaeda in Iraq who was arrested two weeks ago had been planning an attack against the football World Cup in South Africa next month. A 30-year-old Saudi, "participated in the planning of a terrorist act in South Africa during the World Cup," said a Baghdad security spokesman. He added that the suspect was in charge of "security" for the terror network in Baghdad, and was in contact with a terrorist leader to organize the plan hatched by Al Qaeda. Source: http://www.nydailynews.com/blogs/warzone/2010/05/al-qaeda-in-iraq-was-planning.html#ixzz0oCT123ot

Fighter jets escort plane to Vancouver. Canadian fighter jets escorted a Cathay Pacific airliner coming from Hong Kong to a safe landing in Vancouver International Airport May 15 following a bomb threat, officials said. Royal Canadian Mounted Police said that passengers had been safely taken off the plane and that nothing of concern had been found in the baggage. ''This incident is being taken very seriously,'' a police spokeswoman said. Canadian F-18 Hornet fighter jets intercepted the Airbus A340 with 283 passengers and 14 crew members aboard and flew alongside it until it landed. ''As a precaution, NORAD fighters escorted the aircraft until it landed safely in Vancouver,'' said North American Aerospace Defense Command spokeswoman. Passengers told CTV News they were not informed of any problems during the flight. One passenger told CTV News the fighters appeared about 80 miles from Vancouver. ''I was scared,'' he said. ''He was near to our plane, very near to our plane.'' Source: http://www.nytimes.com/aponline/2010/05/15/world/AP-CN-Canada-Plane-Threat.html?_r=1&partner=rss&emc=rss

European airports begin to reopen. Heathrow and Gatwick airports began reopening Monday after a new cloud of ash from a volcano in Iceland prompted aviation authorities in Britain, Ireland and the Netherlands to close much of their airspace for several hours. A spokesman for Schiphol Airport said flights to and from Amsterdam's main international airport would also resume from 2 p.m. local time,

although major disruptions were expected to last throughout the day. Eurocontrol, the agency in Brussels charged with coordinating European air traffic management, said it expected roughly 1,000 flights would be canceled Monday out of around 29,000 that would normally take place this time of year. Winds were dispersing the cloud and reducing concentrations to levels that regulators and engine manufacturers have agreed are safe for commercial traffic. Eurocontrol said the densest parts of the cloud over Europe were at relatively low altitudes, which meant that while take-offs and landings were being disrupted, overflights of the affected areas were still possible. According to the Volcanic Ash Advisory Center in London, the ash plume from Iceland's Eyjafjallajokull volcano was so far remaining below 29,000 feet, while the standard cruising altitude for aircraft is 32,000 to 35,000 feet. Airspace over London Heathrow was closed from 1 a.m. to 7 a.m. Monday. The restriction also included Gatwick and London City Airports and all airfields in Northern Ireland and parts of Scotland. Amsterdam and Rotterdam airports were also shuttered as of 6 a.m. The shutdowns came a month after an ash cloud disrupted most air travel in Europe for nearly a week, forcing the cancellation of thousands of flights, stranding passengers, damaging the continent's economy and raising questions about the oversight of Europe's air traffic. Source:
http://www.nytimes.com/2010/05/18/world/europe/18ash.html?partner=rss&emc=rss

Ukrainian arrested in India on TJX data-theft charges. A Ukrainian national has been arrested in India in connection with the most notorious hacking incident in U.S. history. He was one of 11 men charged in August 2008 with hacking into nine U.S. retailers and selling tens of millions of credit card numbers. He was arrested in India last week, according to a spokesman with India's Central Bureau of Investigation (CBI). The CBI said they had arrested him in New Delhi on the night of May 8, as he deplaned from a flight from Goa, for layover before a flight to Turkey. U.S. authorities had asked for his extradition via diplomatic channels. Known online as "Fidel," the suspect allegedly sold credit card data on an online forum called DumpsMarket, but he was also active on other forums. Source:
http://www.itworld.com/security/107774/ukrainian-arrested-india-tjx-data-theft-charges

Banking and Finance Industry

Bill passed in Senate broadly expands oversight of Wall St. The U.S. Senate May 20, approved a far-reaching financial regulatory bill putting Congress on the brink of approving a broad expansion of government oversight of the increasingly complex banking system and financial markets. The legislation is intended to prevent a repeat of the 2008 financial crisis, but also reshapes the role of numerous federal agencies and vastly empowers the Federal Reserve in an attempt to predict and contain future debacles. The vote was 59 to 39, with four Republicans joining the Democratic majority in favor of the bill. Two Democrats opposed the measure, saying it was still not tough enough. Democratic Congressional leaders and the U.S. President must now work to combine the Senate measure with a version approved by the House in December, a process that is expected to take several weeks. While there are important differences — notably a Senate provision that would force big banks to spin off some of their most lucrative derivatives business into separate subsidiaries — the bills are broadly similar, and it is virtually certain that Congress will adopt the most sweeping regulatory overhaul since the aftermath of the Great Depression. Source:
http://www.nytimes.com/2010/05/21/business/21regulate.html

Twitter malware campaign features a banking Trojan and keylogger combo. A malware campaign that uses fake Twitter accounts and sends out messages marked with popular hashtags, containing

the text “haha this is the funniest video ive ever seen” and a malicious shortened link, has been launched. The messages pop-up when users search for trending topics. The shortened links in the messages all point to a Web page that hosts a Java exploit whose goal is to drop a keylogger/banking Trojan on the visiting computer. F-Secure advises everybody who does not need Java in their browser to disable it, making this kind of attack misses its mark. Source: http://www.net-security.org/malware_news.php?id=1349

Smart credit cards arrive in U.S. — finally. Credit cards featuring smart-card technology have been standard fare around the world for several years now — but not in the U.S., where financial institutions have continued using cards based on less-secure magnetic stripe technology. That may finally be about to change. Last week, the United Nations Federal Credit Union (UNFCU) became the first financial institution in the U.S. to unveil plans to issue credit cards that comply with the Europay MasterCard Visa (EMV) smartcard standard. The credit union’s new Platinum Visa EMV cards will be issued to about 5,000 of its most high-value customers and can be used anywhere EMV cards are accepted. Cards based on the EMV standard use an embedded microprocessor instead of a magnetic stripe to store cardholder data and all of the other information needed to use the card for a transaction. Many financial institutions that issue EMV Chip cards also require cardholders to enter a Personal Identification Number (PIN) as an added security measure when using the card. Chip-and-PIN credit cards are considered to be significantly safer than cards with magnetic stripes, which has led to the widespread adoption of EMV smartcards across Europe and in several other countries. EMVCo, an organization run by MasterCard, Visa, American Express and others to administer the EMV standard, estimates that close to a billion EMV cards were in use worldwide in 2009. Source: http://www.computerworld.com/s/article/9176936/Smart_credit_cards_arrive_in_U.S._finally

US regulators form plans to encourage banks to better protect customers from online fraud. A panel of regulators in the U.S. are drafting plans to force banks to protect their customers better from a surge in online account fraud. According to a report in the Financial Times (FT), a panel with representatives from the FDIC, the Federal Reserve System and other agencies is reacting to the rapid evolution of malicious computer programs designed to drain accounts. Among its plans is to require financial institutions to contact customers through means beside the Internet, following European banks actions in placing calls to clients’ mobile phones to ensure that they intend to transfer money. The FT report also claimed that banks were warned in 2005 not to rely merely on user names and static passwords, which has led to U.S. institutions adopting two-factor authentication for big depositors. However, directives from the FDIC and others have allowed banks to skip that step if they had multiple layers of security checks to flag suspicious money movement. Source: http://www.scmagazineuk.com/us-regulators-form-plans-to-encourage-banks-to-better-protect-customers-from-online-fraud/article/170494/

Teach a man to phish... Phishing may not be the most sophisticated form of cyber crime, but it can be a lucrative trade for those who decide to make it their day jobs. Indeed, data secretly collected from an international phishing operation over 18 months suggests that criminals who pursue a career in phishing can reap millions of dollars a year, even if they only manage to snag just a few victims per scam. Phishers often set up their fraudulent sites using ready-made “phish kits” — collections of HTML, text and images that mimic the content found at major banks and e-commerce sites. Typically, phishers stitch the kits into the fabric of hacked, legitimate sites, which they then outfit with a “backdoor” that allows them to get back into the site at any time. About a year and a half ago,

investigators at Charleston, South Carolina based PhishLabs found that one particular backdoor that showed up time and again in phishing attacks referenced an image at a domain name that was about to expire. When that domain finally came up for grabs, PhishLabs registered it, hoping that they could use it to keep tabs on new phishing sites being set up with the same kit. The trick worked: PhishLabs collected data on visits to the site for roughly 15 months, and tracked some 1,767 Web sites that were hacked and seeded with the phishing kit that tried to pull content from the domain that PhishLabs had scooped up. When PhishLabs plotted the guy's daily online activity, the resulting graph displayed like a bell curve showing the sort of hourly workload a person would typically see in a regular 9-5 job, a researcher said. "In the middle of the day he's super busy, and in the mornings and evenings he's not. So this is very much his day job." Source: http://krebsonsecurity.com/2010/05/teach-a-man-to-phish/

U.S. bank failures inch to 72. On May 14, four more banks were shuttered by U.S. regulators. The failed banks were based in Georgia, Illinois, Michigan and Missouri. This brings the total number of bank failures to 72 so far in 2010, compared to 140 in 2009, 25 in 2008 and 3 in 2007. Although the economy is showing signs of a gradual recovery with large financial institutions stabilizing, tumbling home prices, soaring loan defaults and a high unemployment rate continue to take their toll on small banks. While many expect the economic recovery to gain momentum soon, there remains lingering concern in the banking industry. Failure of both residential and commercial real estate loans as a result of the credit crisis has primarily hurt banks. As the industry tolerates bad loans made during the credit explosion, the trouble in the banking system goes even deeper, increasing the possibility of more bank failures.â_¨â_¨The failed banks are: Saint Marys, Georgia-based Satilla Community Bank with total assets of $135.7 million and deposits of $134.0 million. Plymouth, Michigan-based New Liberty Bank with about $101.8 million in deposits and $109.1 million in assets. Springfield, Missouri-based Southwest Community Bank with about $102.5 million in deposits and $96.6 million in assets. Elmwood Park, Illinois-based Midwest Bank and Trust Company with total assets of $3.17 billion and deposits of $2.42 billion. Source: http://www.zacks.com/stock/news/34243/U.S.+Bank+Failures+Inch+to+72

Chemical and Hazardous Materials Sector

Miniature nuclear plants seek approval to work in U.S. Manufacturers of refrigerator-sized nuclear reactors will seek approval from U.S. authorities within a year to help supply the world's growing electricity demand. The chief executive officer of Hyperion Power Generation Inc., intends to apply for a license "within a year" for plants that would power a small factory or town too remote for traditional utility grid connections. The Santa Fe, New Mexico-based company and Japan's Toshiba Corp. are vying for a head start over reactor makers General Electric Co. and Areva SA in downsizing nuclear technology, and aim to submit license applications in the next year to U.S. regulators. They are seeking to tap a market that has generated about $135 billion in pending orders for large nuclear plants. "We're building iPhones when the nuclear industry has traditionally built mainframe computers," said the CEO. Hyperion has more than 150 purchase commitments from customers such as mining and telecom companies, provided its technology gets licensed for operation, he said. A generation after the Chernobyl and Three Mile Island accidents wiped reactor construction off the agenda of many governments, developers are pressing ahead with designs to satisfy demand for power that doesn't pollute the skies. Source: http://www.bloomberg.com/apps/news?pid=20601109&sid=aNWxvJD2xhZ8&pos=14

EPA adds more than 6,300 chemicals and 3,800 chemical facilities to public database. The U.S. Environmental Protection Agency (EPA) has added more than 6,300 chemicals and 3,800 chemical facilities regulated under the Toxic Substances Control Act (TSCA) to a public database called Envirofacts. The Envirofacts database is EPA's single point of access on the Internet for information about environmental activities that may affect air, water and land in the U.S and provides tools for analyzing the data. It includes facility name and address information, aerial image of the facility and surrounding area, map location of the facility, and links to other EPA information on the facility, such as EPA's inspection and compliance reports that are available through the Enforcement Compliance History Online (ECHO) database. EPA is also adding historic facility information for another 2,500 facilities. EPA has conducted a series of aggressive efforts to increase the public's access to chemical information including reducing confidentiality claims by industry, and making the public portion of the TSCA inventory available free of charge on the agency's Web site. EPA intends to take additional actions in the months ahead to further increase the amount of information available to the public. Source: http://yosemite.epa.gov/OPA/ADMPRESS.NSF/d0cf6618525a9efb85257359003fb69d/b6e361b52038099485257726004e5a98!OpenDocument

Commercial Facilities

(Florida) **Brevard officials frustrated over bomb threats.** Investigators say a 48-year-old homeless man has made more than 30 bomb threats and believe he may be tied to numerous threats made May 19. Even though he is homeless, investigators said the man is able to make calls from cell phones and has been able to block those calls from being traced. But investigators discovered that the suspect has been able to use two different phones, and continue to try to track them. They also believe he is simply using a phone book to access numbers to the different businesses. Agents say another complication is the fact the suspect has no family in the area. One thing has changed in how police are approaching the investigation: they recognize his voice; so not every bomb-threat call has prompted evacuations. Source: http://www.myfoxorlando.com/dpp/news/brevard_news/051910brevard-officials-frustrated-over-bomb-threats

New rule for contractors to prevent lead contamination. As of April 22, 2010, contractors must be certified and follow specific work practices to prevent lead contamination when performing renovation, repair and painting projects in housing and child-occupied facilities built before 1978. The new U.S. Environmental Protection Agency (EPA) rule is aimed at preventing lead poisoning in children and adults and applies to renovation, repair and painting projects that disturb more than six square feet of potentially contaminated lead-based painted surfaces. What the rule will certainly do is directly affect the wallets of contractors, homeowners, property managers and municipalities alike. To comply with the rule, renovation contractors, painters, maintenance workers in multi-family housing, and workers in other specialty trades can expect to incur direct costs of $315 for a one-day certification course. The certification course trains workers on how to contain the work area, minimize dust and perform thorough clean up. Additional contractor costs include $300 for the EPA certification, as well as costs for any new equipment, such as respirator cartridges and HEPA vacuum filters. Non-compliance can be significantly more expensive at $37,500 per day per violation. For homeowners, schools, childcare facilities and others, the additional time and labor associated with

lead-contamination prevention will increase the cost to repair, renovate or remodel. This could lead some to hire uncertified contractors or avoid needed repairs altogether. Source: http://www.reedconstructiondata.com/news/2010/05/new-rule-for-contractors-to-prevent-lead-contamination/

Parking attendants trained to watch for terrorists. A new government program aims to train thousands of parking industry employees nationwide to watch for and report anything suspicious. Organizers said parking attendants and enforcement officers are as important to thwarting attacks as the two Times Square street vendors who alerted police to a smoking SUV that was found to contain a gasoline-and-propane bomb. The program has been in the works for about a year and gave its first presentation at the convention, attended by hundreds of people who run parking operations for cities, universities, stadiums and other places around the country. Funded by the Federal Emergency Management Agency and administered by TSA, the program teaches parking-lot operators to watch for odd activities that could precede an attack by days or months: strange odors such as diesel from gasoline vehicles, cars parked where they shouldn't be, people who seem to be conducting surveillance by taking photos or drawing sketches. The program is part of a larger effort by the government since 9/11 to enlist ordinary people — airline passengers, subway riders, bus drivers, truckers, doormen, building superintendents — to serve as the eyes and ears of law enforcement. The executive director of corporate security for MGM Mirage, which owns all or part of 11 casino-resorts on the Las Vegas Strip, said all new hires, including parking valets, housekeepers, and casino cashiers, are trained to watch for signs of terrorism. Source: http://news.yahoo.com/s/ap/20100514/ap_on_bi_ge/us_parking_lots_terrorism

Communications Sector

FCC waivers and funding could fuel nationwide public safety network. The FCC took a significant step toward building a nationwide public safety network last week by clearing the way for 21 cities, counties and states to begin building their own fourth-generation wireless networks. The commission gave conditional approval May 12 to waiver requests from New Jersey, Los Angeles County, Boston and 18 other entities to start creating 4G networks known as Long Term Evolution (LTE) networks. These networks could begin to form a nationwide interoperable wireless network that has been sought by public safety officials since September 11, 2001 terrorist attacks on the U.S. The FCC's National Broadband Plan calls for creating a nationwide public safety network within the 700 MHz D Block of radio spectrum formerly used by television broadcasters. In 2008, the commission attempted to auction the D Block spectrum to commercial telecom providers, with the winner required to build a nationwide network and share it with public safety agencies. But there were no takers, and a new D Block auction is not expected until 2011. The LTE networks approved last week will use 10 MHz of spectrum that public safety was granted in 1997. But the FCC required that the new networks be compatible with the proposed national D Block 700 MHz network. Source: http://www.govtech.com/gt/articles/763523

Delta IV GPS IIF-01 launch set May 20. The U.S. Air Force will launch the first Global Positioning System Block IIF satellite aboard a United Launch Alliance Delta IV Evolved Expendable Launch Vehicle from Space Launch Complex 37 in Cape Canaveral, Florida May 20. The GPS IIF system brings next-generation performance to the constellation. The GPS IIF vehicle is critical to U.S. national security and sustaining GPS constellation availability for global civil, commercial and defense

applications. Besides sustaining the GPS constellation, IIF features increased capability and improved mission performance and longevity. Not only is it the first IIF to be launched, this will be the first GPS satellite to ride on the Delta IV launch vehicle. Source:
http://www.gpsdaily.com/reports/Delta_IV_GPS_IIF_01_Launch_Set_May_20_999.html

Five ways to (physically) hack a data center. A company can spend millions of dollars on network security, but it is all for naught if the data center has physical weaknesses that leave it open to intruders. Red team experts hired to social engineer their way into an organization said they regularly find physical hacking far too easy. A senior security consultant with Trustwave's SpiderLabs, said data centers he has investigated for security weaknesses commonly have the same cracks in the physical infrastructure that can be exploited for infiltrating these sensitive areas. The five simplest ways to hack into a data center are by crawling through void spaces in the data-center walls, lock-picking the door, "tailgating" into the building, posing as contractors or service repairman, and jimmying open improperly installed doors or windows. Source:
http://www.darkreading.com/database_security/security/management/showArticle.jhtml?articleID=224900081

FTC asked to investigate Google Wi-Fi 'snooping'. A consumer group has called on the U.S. Federal Trade Commission (FTC) to investigate Google after the search company revealed that it had been collecting people's Internet communications from open wireless networks. On May 14, Google said it would stop its Street View cars from sniffing wireless networks after discovering that they had been collecting unencrypted content — the contents of Web pages, for example — unbeknownst to Google. Consumer Watchdog said the FTC should find out exactly what Google logged, how long it collected the information and what it ended up doing with it. "Google has demonstrated a history of pushing the envelope and then apologizing when its overreach is discovered," the group said Monday in a press release. "Given its recent record of privacy abuses, there is absolutely no reason to trust anything the Internet giant claims about its data collection policies." Google was collecting the Wi-Fi data — SSID (Service Set Identifier) information and MAC (Media Access Control) addresses — in order to get better location information for its Google Maps service. Source:
http://www.computerworld.com/s/article/9176902/FTC_asked_to_investigate_Google_Wi_Fi_snooping_

One in four U.S. homes now cell-only. One in four U.S. homes is now cellphone-only, according to figures for the second half of 2009. A further 14.9 percent of homes receive all or almost all calls on mobiles, despite having a landline, meaning that 89 million U.S. adults (nearly two in five) are now cell-only or 'cell-mostly'. "The potential for bias due to undercoverage remains a real and growing threat to surveys conducted only on landline telephones," said the latest report from the National Center for Health Statistics (NCHS), which conducts continuous research on health-related behaviors, as well as landline and cellphone usage. Many research organizations are beginning to sample cell-only homes alongside landlines, or to use address-based sampling for telephone fieldwork. The number of cell-only homes has risen steadily from less than 3 percent when NCHS first started collecting the data in 2003. The latest figure shows a rise of 4.3 percentage points from the same period in 2008, roughly the same rate at which it rose in the 12 months before that. Source:
http://www.research-live.com/news/one-in-four-us-homes-now-cell-only/4002704.article

Crime friendly ISP offline. A cyber crime friendly Internet service provider (ISP) was knocked offline Friday after its upstream provider had its service cut off, according to Zeus Tracker. PROXIEZ-NET, a Russian based ISP that hosted at least 13 known Zeus command and control channels, lost its connection after its upstream provider, DIGERNET, had its Internet connection cut. It was withdrawn from Internet routing tables, according to an AS Report. PROXIEZ-NET has often been accused of being a haven for cyber criminals. It is unclear how this will impact the botnets that utilize PROXIEZ-NET, as previously disrupted servers have merely found new hosts to reconnect with the infected computers they control. Source: http://www.thenewnewinternet.com/2010/05/17/crime-friendly-isp-offline/

Defense Industrial Base Sector

U.S. agrees to announce missile launches. The U.S. has agreed to notify other nations before it launches most ballistic missile tests or satellites, in a measure that builds on a landmark arms agreement with Russia and is meant to encourage Moscow to reciprocate. The American decision was contained in a confidential note made available Thursday to The Associated Press and confirmed by three diplomats familiar with the issue. The move is less far-reaching or binding than the treaty signed last month by the U.S. and Russian presidents that outlines cuts in both nations' massive nuclear arsenals. But it is significant in reflecting Washington's determination to build on the success of that agreement. For years, Russia voluntarily provided such pre-notifications regarding the launch of ballistic missile tests or satellites. But it stopped doing that two years ago, complaining that the U.S. and other nations were not following suit. One senior diplomat familiar with the issue said that Moscow is now expected to resume its reporting. That would add to the confidence building that received a huge push with last month's signing of the nuclear arms agreement. "The United States ... will provide pre-launch notification of commercial and National Aeronautics and Space Administration (NASA) space launches as well as the majority of intercontinental ballistic and submarine-launched ballistic missile launches," said the note forwarded to HCOC, an organization overseeing efforts to curb the spread of such weapons. Source: http://www.militarytimes.com/news/2010/05/ap_missiles_launch_052010/

M-4 not suited to warfare in Afghan hills. The U.S. military's workhorse rifle is proving less effective in Afghanistan against the Taliban's more primitive but longer range weapons. As a result, the U.S. is re-evaluating the performance of its standard M-4 rifle and considering a switch to weapons that fire a larger round largely discarded in the 1960s. The M-4 is an updated version of the M-16, which was designed for close quarters combat in Vietnam. It worked well in Iraq, where much of the fighting was in cities such as Baghdad, Ramadi and Fallujah. But an Army study found that the 5.56mm bullets fired from M-4s don't retain enough velocity to kill an adversary at distances greater than 1,000 feet. In hilly regions of Afghanistan, NATO and insurgent forces are often 2,000 to 2,500 feet apart. Afghans have a tradition of long-range ambushes against foreign forces. During the 1832-1842 British-Afghan war, the British found that their Brown Bess muskets could not reach insurgent sharpshooters firing higher-caliber Jezzail flintlocks. Soviet soldiers in the 1980s found that their AK-47 rifles could not match the World War II-era bolt-action Lee-Enfield and Mauser rifles used by mujahedeen rebels. The heavier bullets enable Taliban militants to shoot at U.S. and NATO soldiers from positions well beyond the effective range of the coalition's rifles. To counter these tactics, the U.S. military is designating nine soldiers in each infantry company to serve as sharpshooters. They are

equipped with the new M-110 sniper rifle, which fires a larger 7.62mm round and is accurate to at least 2,500 feet. Source: http://www.militarytimes.com/news/2010/05/ap_m4_052110/

Army formally cancels missile program. The Army has formally canceled the Non-Line of Sight-Launch System, a billion-dollar missile program under development by Tucson, Arizona-based Raytheon Missile Systems and Lockheed Martin. The Navy is still evaluating its options for the system, which it had been considering for use aboard a new line of coastal combat vessels. The modular system, known as NLOS-LS or simply NLOS, features 15 all-weather missiles in a common launcher that can be mounted on an array of military vehicles. The NLOS-LS was part of the Army's Future Combat Systems program, which was canceled last year. Raytheon makes the NLOS-LS's Precision Attack Missile (PAM) and Lockheed Martin makes the launch unit, under a joint venture called Netfires LLC. "It's disappointing that the U.S. Army has decided to cancel the NLOS-LS program," Raytheon said in a prepared statement to the Star. "After a more than $1 billion investment over ten years, the program stands at 92 percent complete." The cancellation comes after recent test failures and an examination of the program by a Pentagon review board, which recommended cancellation last month. The missile failed in four of six flights in a critical Army "limited user test" at White Sands Missile Range in New Mexico in late January and early February. The missile had succeeded in 12 of 17 prior tests, and Raytheon said the recent problems have been fixed. Source: http://azstarnet.com/business/local/article_27505ee7-bcb2-5fb4-a5bb-6ee1a9cde68e.html

Northrop: Ford's design issues minimal. Engineers building the new aircraft carrier Gerald R. Ford (CVN 78) are making some design changes to avoid "electrical cable routing issues" that could interfere with some internal arrangements. The problems have been found "in limited areas of the ship design," said a spokesperson for Northrop Grumman Shipbuilding. "As can happen with any lead ship of the class performing first-of-a-kind activities, we have identified some interferences between cable arrangements and other design features that require correction. In these cases, changes to the design are being made and lessons learned applied," the spokeswoman said. Those changes include moving some wireways where electrical cable is strung and changing some cable supports, she added. "These issues are not widespread. We have not yet run any cable, but a small percentage of the cable supports that have been installed may require alteration." The impact on the ship's cost or construction schedule is still being evaluated, she said, "but expect it to be minimal." The Navy's Sea Systems Command (NAVSEA) acknowledged the problem but downplayed the impact. "The Navy is aware that [Northrop Grumman Shipbuilding] has identified some interferences between cable arrangements that require correction," NAVSEA said in an e-mail statement May 14. "The Navy understands this to be a small percentage of the cable arrangement design to date and results in no module fit-up issues." The ship, first of a new class of carriers, is under construction at Northrop's shipyard in Newport News, Va. More than 61 percent of the structural modules for the Ford are already complete, the spokeswoman said. "The fit-up of CVN 78 structural modules is as good or better than previous Nimitz-class carriers," she added. Source: http://www.militarytimes.com/news/2010/05/navy_defense_ford_electrical_051810w/

(Connecticut; New York) **Source: Faisal Shahzad had bigger targets.** A source close to the Times Square-bomber investigation said that the suspect had bigger, more destructive plans — other targets in New York and Connecticut. The source said that the suspect has told interrogators that if the Times Square bombing was successful, that he had four other locations to possibly attack. If the bomb inside the Nissan Pathfinder in Times Square went off as planned, a source said that the

bomber said he was taking aim at four other high-profile targets: Connecticut-based defense contractor Sikorsky, Rockefeller Center, Grand Central Terminal, and the World Financial Center across from Ground Zero. Sikorsky manufacturers helicopters for the U.S. military, including the Blackhawk. Headquartered in Stratford, Sikorsky also has facilities in Shelton and Bridgeport — the same two cities where the bomber has lived. Source: http://www.myfoxny.com/dpp/news/international/source-faisal-shahzad-had-bigger-targets-20100517

Corps works to lengthen lives of old CH-53s. Marine officials are working overtime to keep the Corps' aging CH-53s flying until the next-generation heavy-lift helicopter comes online in 2018, three years later than expected. The program manager for all CH-53s, said his team is on track to conduct the CH-53K's critical design review this summer. That will be the last major step before the new aircraft is approved for production. Officials hope to have the first new bird conducting flight tests in 2013. In the meantime, the Corps will ask even more of its CH-53Ds and Es. "I think we're going to be fine," the manager said, but it would be "foolhardy not to be concerned about an aging aircraft. We have to be diligent. ... If we don't do anything, we could be in trouble in the next five years or less." A diagnostic system on board the older aircraft helps Marine officials track the bird's reliability. Typically, mechanical failure doesn't happen overnight, the manager said. Officials hope the data collected from the diagnostics will help them predict when failure is most likely to occur. Additionally, officials have determined that if they replace the bulkhead in the tail of the CH-53Es before they reach 6,190 flight hours, they can keep them flying to 10,000 hours. Engineers also have discovered that extra maintenance on the Delta models can extend the aircraft's lifespan to 12,500 hours, so long as the work is completed before the bird hits 10,000 hours, the manager said. Source: http://www.militarytimes.com/news/2010/05/marine_ch53k_051610w/

Critical Manufacturing

BMW brake recall: the official word. BMW Motorrad has announced the recall of R-Series boxer-twin and K 1200 GT motorcycles, manufactured between August 2006 and May 2009, after a potential fault in a brake pipe was diagnosed. It is possible that vibrations on affected motorcycles could cause the front brake pipe to leak and, over an extended period of time, cause brake fluid to escape. BMW Motorrad sought to reassure customers that the number of motorcycles, in which leaking brake pipes was noticed, is very small (one-tenth of a percent). No accidents have arisen as a result of this fault. In the event of a problem, riders will notice the leaking brake fluid or a reduction in the brake fluid level in the handlebar mounted brake fluid reservoir. This may result in a gradual loss of braking performance of the front brake. The rear brake is not affected. The BMW Motorrad dealer network plans to contact all customers who own motorcycles potentially affected by this fault. Source: http://www.visordown.com/motorcycle-news--general-news/bmw-brake-recall-the-official-word/11495.html

Toyota pays $16.4M fine for slowness in pedal case. Toyota Motor Corp. paid a record $16.4-million fine yesterday for a slow response in its accelerator pedal recall. A Transportation Department official said the Japanese automaker paid the fine after reaching an agreement with the government April 19. Toyota had 30 days to pay it. The official was not authorized to speak publicly before an announcement was made. Toyota faced the maximum penalty allowed under law after it was accused of hiding earlier defects involving gas pedals. Toyota rejected the accusation even though it

agreed to pay the fine. The world's largest car manufacturer has recalled more than 8 million vehicles worldwide for safety defects that affect some of its best-selling models. The company still faces hundreds of state and federal lawsuits in the United States. The Transportation Department is reviewing thousands of Toyota documents and could issue penalties over the company's handling of other safety recalls. Toyota confirmed paying the fine but declined further comment. Source: http://toledoblade.com/article/20100519/BUSINESS02/5190335/-1/BUSINESS

2010 Nissan Altimas recalled. Nissan is recalling a small number of 2010 Altimas because some structural welds may be out of specification, which could affect vehicle crash performance. Dealers will inspect the vehicles and, if necessary, repair them free of charge. The affected units were assembled from April 7, 2010 through April 13, 2010. Source: http://www.consumeraffairs.com/recalls04/2010/2010_altima.html

2008-2010 Volvo XC70 recalled. Volvo is recalling certain XC70 models from the 2008 through 2010 model years. The affected models contain incorrect tire inflation information. Dealers will inspect the vehicles and, if necessary, install a new tire and loading information label and tire-pressure management software. The owners manual will also be updated. Source: http://www.consumeraffairs.com/recalls04/2010/volvo_xc70.html

2010 Chrysler, Dodge, Jeep models recalled. Chrysler is recalling about 40,000 Chrysler, Dodge and Jeep models from the 2010 year. The vehicles may have a defective ignition switch that would allow the key to be removed prior to placing the shifter in the "park" position. This could lead to unintended vehicle movement. The affected models are: 2010 Chrysler 300, 2010 Dodge Challenger, 2010 Dodge Charger, 2010 Dodge Ram, 2010 Jeep Commander, and 2010 Jeep Grand Cherokee. Dealers will inspect the ignition module and replace defective units free of charge when the recall begins in July 2010. Source: http://www.consumeraffairs.com/recalls04/2010/chrysler_ignition.html

2010 Subaru Legacy, Outback recalled. Subaru is recalling nearly 30,000 Legacy and Outback vehicles from the 2010 model year. The CVT cooler hose can split, resulting in a fluid leak, which could cause the car to come to an unexpected stop. Subaru will notify owners and dealers will replace any defective hoses free of charge. Source: http://www.consumeraffairs.com/recalls04/2010/2010_subaru.html

(Kentucky) **Suspicious package empties Toyota.** Hundreds of employees at a northern Kentucky Toyota engineering facility were evacuated after officials were called in to investigate a suspicious package delivered to the mailroom. A spokeswoman for Toyota Motor Engineering and Manufacturing North America said the May 14 incident lasted about two and a half hours and the package was determined to be harmless. The spokesman said between 900 and 1,000 people work at what is known as TEMA in Erlanger. She said employees were allowed to go home but many stayed and returned to work once they were allowed back inside the building. A supervisor in the FBI's Covington office, said FBI agents were called to the scene along with local law enforcement agencies. Source: http://www.wbko.com/news/headlines/93915944.html

Emergency Services

(Florida) **Vandalism damages crucial Coast Guard communications in Palmetto.** Authorities are seeking information on vandalism that occurred at a crucial communication hub for the U.S. Coast Guard in Palmetto, Florida, according to a Coast Guard report. On May 16 at 11:30 p.m., Coast Guard officials in St. Petersburg lost power to a VHF communications system at its Palmetto facility, which handles crucial distress signals for the area. Upon investigation, authorities found that the system and a generator had been purposely damaged. "This particular incidence of vandalism degraded the Coast Guard's VHF communications system and potentially compromised public safety," a statement released by the Coast Guard said. Source: http://www.bradenton.com/2010/05/20/2301150/vandalism-damages-crucial-coast.html

Bill would require FBI to fill in gaps in criminal records database. A bill introduced in the U.S.House of Representatives would strengthen the accuracy of the FBI's criminal records database by requiring the U.S. Attorney General's Office to verify that crime data is up to date. Employers rely on the database to conduct background checks on potential hires. The 2010 Fairness and Accuracy in Employment Background Checks Act would require the Attorney General to find out from court offices, including those in state and local jurisdictions, the outcome of arrests whenever an employer requests a background check, and update that record in the National Crime Information Center database. In cases where the Attorney General discovers an arrest was dismissed in court, he has 10 days to update the record before responding to the employer's request. Employers often consult the NCIC database to conduct background checks on individuals applying for jobs in law enforcement, homeland security or organizations where they would be working with vulnerable populations, such as children and the elderly. Typically only public sector entities can request FBI background checks, though certain private sector companies — such as those supporting federal homeland security efforts — can as well. Source: http://www.nextgov.com/nextgov/ng_20100518_2029.php?oref=topnews

(Michigan) **Police under investigation.** The Muskegon Heights Michigan Police Department is under investigation for its sloppy handling of evidence, some of which may be missing. The acting police chief has asked state troopers to do an independent audit of their evidence locker because it appears some money has disappeared. The prosecutor said the evidence room is a shambles with poor organization and poor recordkeeping. He said unlike most departments that destroy drugs and remove cash when cases are prosecuted, in Muskegon Heights it was left lying around. The interim chief requested the audit and then resigned. Source: http://www.wtvbam.com/news/articles/2010/may/13/police-under-investigation/

Energy

(Idaho) **DOE approves $2-billion loan for Areva's nuclear facility in Idaho Falls.** The U.S. Department of Energy Thursday approved a $2-billion loan guarantee for the French company Areva to build a nuclear power facility near Idaho Falls, Idaho The proposed $3.3-billion facility, called the Eagle Rock

Uranium Enrichment Plant, could lead to 400 permanent jobs and up to 1,000 jobs to build the plant, and bolster the state's nuclear energy efforts. The Idaho governor applauded the move. "The loan guarantee confirms that Idaho continues to lead the nuclear renaissance in America," he said in a news release. "The decision also paves the way for new careers and economic recovery across the state." The governor had written to the federal energy department asking them to approve the loan for Areva, and mentioned the plant in Idaho Falls during campaign appearances. Areva still must obtain a license from the Nuclear Regulatory Commission before it can begin construction of the facility. Source: http://www.idahoreporter.com/2010/doe-approves-2-billion-loan-for-areva%E2%80%99s-nuclear-facility-in-idaho-falls/

(Missouri) **Man charged in attempted theft of copper from KC electrical substation.** Kansas City police arrested a 38-year-old man Thursday after he and another man allegedly tried to steal copper from a Kansas City Power & Light substation. The thieves didn't get any copper but caused an estimated $10,000 in damage, police said. Two men entered a fenced area and used bolt cutters to cut copper from electrical transformers and other equipment. Security guards called police, who arrived while the thieves were on the scene. They ran, but officers caught one. A ground wire had been pulled up and cut away from the ground, police said. Several other pieces of copper wire had been cut away from a transformer tower. Officers also found a hole in the fence. Source: http://www.kansascity.com/2010/05/20/1960084/man-charged-in-attempted-theft.html

Food and Agriculture

USDA study shows gaps in local meat infrastructure. A preliminary study revealed by the U.S. Department of Agriculture (USDA) May 20 maps exactly where gaps exist in the local meat-processing infrastructure by showing the availability of slaughter facilities for small and very small producers. The maps were released yesterday during an agency briefing on the "Know Your Farmer, Know Your Food" initiative, which recently took some heat from Republicans in the U.S. Senate. Yesterday's briefing was meant to clarify the initiative's goals and provide details on various inter-agency-coordinated projects. According to the USDA, the assessment of slaughter availability was done to identify regions with "relatively high densities of small livestock and poultry producers, but without a nearby slaughter facility," so that eventually assistance can be provided to existing and new facilities. Supporting slaughter availability for small livestock and poultry producers will benefit both local food systems and the public health, the agency said. When asked whether USDA's initiative to support local meat infrastructure will lead to an increase in the number of meat inspectors, the director of program evaluation and improvement at the Food Safety and Inspection Service (FSIS) told Food Safety News that the agency "hadn't gotten to that point yet," as the initiative is just beginning. Source: http://www.foodsafetynews.com/2010/05/usda-study-shows-gaps-in-local-meat-infrastructure/

Team diarrhea: A model for food detectives around the country. After Minnesota played a huge role in solving two of the nation's major salmonella outbreaks, some federal lawmakers want to duplicate the state's approach to handling food-borne illnesses. A Democratic Minnesota Senator is co-sponsoring legislation that would create four or five centers of excellence around the country to investigate suspected food safety problems, like salmonella and E. coli. The centers would be modeled after Minnesota, which requires doctors to report all suspected cases of food-borne illness to the state Department of Health. Each confirmed case is quickly investigated by University of

Minnesota graduate students, who are known as "Team Diarrhea" or "Team D." They call the patients and ask a series of questions about their symptoms and the food eaten before getting sick. Their investigative work last year helped solve a major peanut butter salmonella outbreak, which killed nine people nationwide, including three from Minnesota. Food safety advocates are also pushing a larger bill — the FDA Food Safety Modernization Act — which would make a series of changes to make America's food system safer. The bill would require more inspections and give the Food and Drug Administration more authority for mandatory recalls. Source: http://www.kare11.com/news/news_article.aspx?storyid=849674

Method found to stop E. coli in cattle. U.S. microbiologists said they have identified a process that might be able to help prevent outbreaks of a food-borne illness caused by E. coli in cattle. Scientists at the University of Texas Southwestern Medical Center, working with the U.S. Department of Agriculture, said they interfered with a genetic sensing mechanism that allows the E. coli strain known as enterohemorrhagic O157:H7, or EHEC, to form colonies within cattle, causing the bacteria to die before reaching the animals' recto-anal junction — the primary site of colonization. Most other strains of E. coli gather in the colon. "We're diminishing colonization by not letting EHEC go where it needs to go efficiently," said an associate professor of microbiology and senior author of the study. "If we can find a way to prevent these bacteria from ever colonizing in cattle, it's possible that we can have a real impact on human disease." She said the finding is important because an estimated 70 percent to 80 percent of U.S. cattle herds carry EHEC. Although EHEC can be a deadly pathogen to humans, the bacterium is part of cattle's normal gastrointestinal flora. The findings are to be reported in the Proceedings of the National Academy of Sciences. Source: http://www.upi.com/Science_News/2010/05/18/Method-found-to-stop-E-coli-in-cattle/UPI-54321274194978/

Pre-cut lettuce is suspected cause of food poisoning outbreak. Bagged lettuce suspected of causing a multi-state outbreak of E. coli illness raises new questions about whether pre-cut produce is riskier than whole vegetables. The outbreak, which involves romaine lettuce cut up and distributed in bags to 23 states and the District, is the latest in a string of recent food-poisoning cases involving pre-shredded leafy greens. The romaine in question was not sold directly to consumers in the produce section but was used by food service companies and supermarkets in salad bars and "grab and go" meals. It is difficult to judge whether pre-cut produce has been linked to more outbreaks than whole vegetables because state and federal health officials don't always specify whether the leafy greens associated with an outbreak were bagged or whole. A senior adviser for produce safety at the Food and Drug Administration said bagged greens represent a disproportionate number of recalls, chiefly because they're easier to identify than whole produce. But, he said, pre-cut produce is not inherently riskier than whole vegetables. The current outbreak is drawing special attention because the romaine lettuce was contaminated with E. coli O145, a strain that is primarily found in cattle and wildlife feces and has never before been linked to a food-borne illness, according to the CDC. The chief of CDC's Enteric Diseases Epidemiology branch said it is likely that E. coli O145 has caused previous food poisonings but has gone undetected because only about 5 percent of clinical laboratories are able to detect it. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/05/17/AR2010051703033.html?hpid=sec-health

Toxic chemical found in canned foods. Eating common canned foods is exposing consumers to levels of bisphenol A (BPA) equal to levels shown to cause health problems in laboratory animals, according

to a new study released today by Illinois PIRG and the National Work Group for Safe Markets, a coalition of public health and environmental groups. The study tested food from 50 cans from 19 U.S. states and one Canadian province for BPA contamination. Over 90 percent of the cans tested had detectable levels of BPA, some at higher levels than have been detected in previous studies. The new study comes as Illinois lawmakers in Springfield consider legislation to eliminate BPA from baby-food packaging. The canned foods tested were brand name fish, fruits, vegetables, beans, soups, tomato products, sodas and milks. The cans were purchased from retail stores and were chosen from report participants' pantry shelves, and sent to an independent laboratory for testing. One can of DelMonte green beans had the highest levels of BPA ever found in canned food, at 1,140 parts per billion. The test results show there is no consistency in the amount of BPA in specific food brands or in types of food, which prevents consumers from being able to avoid BPA canned foods just by looking at a label. For example, two different cans of the same brand of peas with two separate "lot numbers" were drastically different: one had six parts per billion of BPA, while the other had over 300 parts per billion of BPA. "Anyone who reads this report would agree that getting BPA out of food is an urgent food safety issue that demands immediate congressional action," said the policy director at the Breast Cancer Fund. Source: http://www.wpsdlocal6.com/news/local/94182714.html

USDA beefs up school meat-safety program. Come fall, the ground beef used in school lunches will be as safe as ground beef sold to the nation's fast food chains — a major improvement, critics say. The U.S. Agriculture Department (USDA) announced May 14 that it will require all ground beef purchased for the National School Lunch Program to adhere to new safety standards after July 1. The program supplies ground beef, chicken and other food for more than 31 million schoolchildren. The rules bring school lunches "right in line with contemporary standards," said a food-safety consultant who developed a rigorous safety program for the Jack in the Box chain. "In fact, I'd make the case that the school lunch standards will now be above some of our major retail grocery chains." The USDA announced in February that it would raise standards for school lunches and has spelled those standards out in detail. The rules call for more stringent microbiological testing and said beef should be sampled every 15 minutes on production lines. Previously, ground beef bound for schools was sampled an average of eight times during an entire production day, and then those samples were combined and subjected to testing once a shift. The rules make suppliers with "a long-term poor safety record" ineligible to sell to the school lunch program without a complete analysis of why their products failed inspections, said a spokesman for the USDA's Agricultural Marketing Service (AMS), which purchases beef for the school lunch program. No currently eligible contractors would be ineligible under that requirement "if it were in effect," he said. Source: http://www.usatoday.com/news/education/2010-05-14-school-meat-safety_N.htm

(Utah) **Nine sickened by campylobacter illness linked to raw milk.** An illness linked to raw milk has infected nine people in Utah. The Utah Department of Health (UDOH) announced May 17 that two dairies in the state, including one in Weber County, had sold contaminated milk that made 15 people ill. Ropelato Dairy at 4019 W. 1800 South in Ogden was the source of the campylobacter outbreak that sickened nine people, according to spokespeople from the Utah Department of Agriculture and UDOH. Raw milk from a dairy in Richfield gave several people salmonella. Raw milk was approved for sale by the Utah Legislature in 2007 despite opposition from the U.S. Department of Agriculture (UDA) because of health concerns, a UDA spokesman said. "Raw milk, no matter how carefully handled, has risks," said a Weber-Morgan Health Department epidemiologist. Now raw milk, which is unpasteurized and goes from cow to refrigeration without treatment, is legally available for retail

only through places permitted by the UDA. The milk is tested monthly for problems, and sales are suspended if bacteria is found, the UDA spokesman said. The milk is then tested weekly until it is within safety standards, when the raw milk can be sold again, he said. The co-owner of Ropelato Dairy, said they stopped selling raw milk after hearing of one person getting sick. He said they are not currently selling the milk and will decide whether to begin selling raw milk again. The Weber-Morgan Health Department epidemiologist said raw milk has made up about a third of the health department's campy cases in the last year. Source: http://www.standard.net/topics/food/2010/05/17/nine-sickened-campylobacter-illness-linked-raw-milk

(Louisiana) **Norovirus may not be cause of Central deaths.** New test results may point to another cause for the deaths of three Central Louisiana State Hospital patients earlier this month. Initial test results led investigators with the Department of Health and Hospitals to believe the common norovirus is what led to more than 40 patients and staff at the Pineville facility getting sick and three patients dying May 7 and 8. But while some patients' stools tested positive for the virus, many did not. Now it is thought that norovirus isn't an "adequate explanation" for the illnesses and deaths, said the medical director for the Alexandria-based Region 6 of the DHH's Office of Public Health. Because of that doubt, a Centers for Disease Control team came to the Pineville behavioral health hospital to intensify the investigation. They stayed through May 17, working with local staff, collecting new samples, re-interviewing patients and staff, re-examining medical records and re-analyzing epidemiological data, the medical director said. He said new samples would be sent off to be tested for even more agents along with samples of all of the food in the kitchen that had been carefully saved and preserved, the medical director said. The medical director said all signs of sickness seem to have subsided, with the last instance of diarrhea occurring four days ago. "Clearly norovirus was there," he said. "The problem is there are a lot of causes of food poisoning. Some are bacterial, some are viral. And norovirus is nearly at the top of this list. But it does not seem to explain all of the cases and is not present enough to feel that it is 100 percent sure the cause of everything." He was unable to give specifics, but did say that not all of the patients who died tested positive for norovirus. The hospital's kitchen remains closed, and it won't reopen until all tests have come back. Once they are completed, the medical director said, the kitchen will undergo a "super cleaning." The hospital's staff has already begun to receive food-handling training. Source: http://www.thetowntalk.com/article/20100518/NEWS01/5180322

(Illinois) **Illinois firm recalls imported beef products due to potential animal-drug contaminant.** Chicago-based Sampco, Inc. is recalling approximately 87,000 pounds of beef products that may contain the animal drug Ivermectin, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced May 14. Ivermectin is a broad-spectrum antiparasitic and is used as a de-worming agent in live animals. The recall involves 12 oz. cans of "Libby's Corned Beef" distributed to retail locations nationwide and 35 lb. boxes of "Seasoned Cooked Beef" distributed to an establishment for further processing. Each product package bears "BRASIL 337 S.I.F" on either the top or the side, as well as "Product of Brazil" or "Packed under Brazilian Government Inspection." The problem was discovered through FSIS routine sampling. Since March 15, 2010, samples from cooked beef products imported from Brazil establishment SIF 337 have resulted in 12 instances of the level of Ivermectin found in the product exceeding the tolerance level established by the Department of Health and Human Service's Food and Drug Administration (FDA) of 10 parts per billion in beef muscle. The production lots that produced violative results were refused entry into the U.S. and are

not available in commerce. However, it was discovered associated products with similar source materials entered the country separately. These are the products that were released into commerce and therefore subject to the recall. The Brazilian firm SIF 337 has been delisted and beef products from that establishment are not permitted entry to the U.S. FSIS is taking additional actions regarding other lots of cooked beef products from Brazil establishment SIF 337 and other manufacturers of cooked beef products from Brazil. FSIS and the company have received no reports of illness or adverse reactions due to consumption of these products. Source: http://www.fsis.usda.gov/News_&_Events/Recall_033_2010_Release/index.asp

(Utah) **Utah unpasteurized milk contained Salmonella.** Several Utah state and county agencies said samples of unpasteurized milk show it contained Salmonella when six people fell ill in Utah, Salt Lake, and Wasatch counties. The Utah Department of Agriculture and Food, Utah Department of Health and Utah County Health Department announced their findings May 14. The sale of unpasteurized, or raw, milk was suspended at stores supplied by the dairy April 23. Testing done on new milk has shown the product meets standards set by Utah law. The dairy was allowed to resume sales May 12. The department of agriculture's director of regulatory services said the agency is working with the dairy to identify the source of the salmonella. Source: http://www.sltrib.com/news/ci_15093270

(California) **California firm recalls ground-beef products due to possible E. coli contamination.** Montclair Meat Co., Inc., a Montclair, California, firm, is recalling approximately 53,000 pounds of ground beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced May 15. The recall covers various pound packages of "Montclair Meat Co. Ground Beef" and "Montclair Meat Co. All Beef Patties." Each package bears establishment number "Est. 6116" inside the USDA mark of inspection. These ground-beef products were produced between the dates of May 3 through May 13, 2010 and were shipped to retailers and federal establishments for further processing in the Los Angeles, California, metropolitan area. The problem was discovered through FSIS microbiological sampling. FSIS has received no reports of illnesses associated with consumption of these products. Source: http://www.fsis.usda.gov/News_&_Events/Recall_034_2010_Release/index.asp

Government Sector (including Schools and Universities)

(Pennsylvania) **Powder scare locks down government building in Center City.** For the second time in two days, a white powder scare shut down a major section of center city Philadelphia. On Friday morning, a city water department employee in the concourse (lower) level of the Municipal Services Building (MSB), across the street from city hall, opened an envelope that contained a yellowish, powdery substance. Other employees immediately called 911 and the area around the MSB was cordoned off by police and firefighters. The MSB, which occupies the block between Broad, 15th, Arch, and JFK Boulevard, was locked down with no one allowed in or out. A haz-mat team performed preliminary tests on the powder, all of which were negative. The two city workers who had come into contact with the powder were evaluated on scene by an EMS crew before being transported to a nearby hospital for further tests. About a half hour later, police were allowing people in and out of the building from the ground level, but the lower concourse level remained closed for an additional 30 minutes. Officials said the powder had been contained with a Philadelphia Water Department bill

in a payment envelope that had apparently been damaged in transit and repackaged by the U.S. Postal Service. One source indicated that the powder may have been a crushed dietary supplement tablet. Source: http://www.kyw1060.com/Another-Powder-Scare/7123038

IG: Poor controls over access to IRS portal put taxpayer data at risk. The Internal Revenue Service (IRS) failed to implement adequate security measures to protect sensitive data that tax professionals entered into a Web portal, according to an inspector general (IG) report released Monday. A fiscal 2009 audit by the Treasury IG for Tax Administration showed tax professionals were able to transfer authorization to access the Registered User Portal to individuals who did not go through the standard checks for tax compliance, past violations of e-file requirements and criminal records. The IRS performs suitability checks when tax firm principals or officials apply for entry, but then allows them to delegate their access rights to others by filing for power of attorney, auditors found. "Taxpayers expect the IRS to protect their personal data, and we believe the power of attorney document does not provide the same assurance as the suitability check," the IG stated. "Any individual can become a delegated user. Many of the delegated users may have questionable backgrounds." The audit found there were 9,988 delegated users permitted to file income-tax returns electronically through the portal. About 6,500 of them also had access to electronic services that enabled them to retrieve and manipulate taxpayer data. In addition, the IRS allows authorized users to assign a special principal consent privilege to a delegated user, which lets that user extend his or her privileges to others. Source: http://www.nextgov.com/nextgov/ng_20100517_2540.php

(Florida) **Security stepped up at Chamberlain High.** Students at Chamberlain High School in Tampa, Florida were greeted by extra security Tuesday morning, one day after a homemade acid bomb went off in a hallway and injured a student, putting the school on lockdown for several hours. Tampa police are providing additional security patrols Tuesday, saying they, along with school officials, are not taking the situation lightly. Authorities said they still have not determined who rolled the chemical-filled, plastic water bottle out of a classroom and into a hallway around 8:30 a.m. Monday. The device exploded, slightly burning an 18-year-old girl. A second acid bomb that did not detonate was found in a nearby bathroom while police were searching the school. Some students told FOX 13 Tuesday morning that they were somewhat hesitant coming to school. Monday, some students speculated that the incident may have been some sort of prank, but school officials said that doesn't matter and that they still plan to prosecute whoever is responsible. Source: http://www.myfoxtampabay.com/dpp/news/local/hillsborough/security-stepped-up-at-chamberlain-high-051810

Survey: Gov't agencies use unsafe methods to transfer files. Employees at many U.S. government agencies are using unsecure methods, including personal e-mail accounts, to transfer large files, often in violation of agency policy, according to a survey. Fifty-two percent of the respondents to the survey of 200 federal IT and information security professionals said employees at their agencies used personal e-mail to transfer files within their agencies or to other agencies. About two-thirds of those responding to the survey said employees used physical media, including USB drives and DVDs, to transfer files, and 60 percent of employees use FTP (File Transfer Protocol), according to the survey, completed by MeriTalk, a government IT social-networking site, and Axway, an IT security vendor. Forty percent of those surveyed said employees at their agencies use virtual private networks to transfer files and 34 percent said employees use Web-hosted, file-transfer services. Sending unencrypted data over FTP or personal e-mail, or putting it on physical media is a major problem for

data security, the survey authors said. In March, the U.S. House of Representatives passed the Secure Federal File Sharing Act, which in many cases would prohibit government employees from using peer-to-peer file-sharing software, including FTP. The bill, sponsored by a Democratic congressman from New York, is awaiting action in the Senate. Source: http://www.computerworld.com/s/article/9176889/Survey_Gov_t_agencies_use_unsafe_methods_to_transfer_files

Aging jets concern retiring NORAD chief. A four-star general who is retiring from the military's top homeland security position said Thursday the nation's radar system needs to be replaced and its jet fighter fleet is getting old. "The aging systems that we use for many of our NORAD missions is a concern for me," said the Air Force general who was the commander of the North American Aerospace Defense Command (NORAD) and the U.S. Northern Command. NORAD is a joint U.S.-Canada command that monitors air and space threats to both nations. Northern Command oversees the U.S. military's homeland defense and supports civilian authorities. Both have headquarters at Peterson Air Force Base in Colorado Springs. At a news conference Thursday, the general said he feels good about the direction of the two commands and is leaving behind "no unfinished business." But the general said the nation's current radar system needs to be updated with an integrated system of sensors that can seamlessly monitor space, maritime areas and U.S. border areas, as well as the air. "The answer isn't just 'fix radar sites,' " the general said. The general also warned that "our air defense alert fighters are aging," a reference to the current fleet of F-16 jets that are sent aloft during potential aerial threats, including disturbances aboard domestic airliners. Many older-model F-16s are flying well past their designed life span after undergoing upgrades. Source: http://www.military.com/news/article/aging-jets-concern-retiring-norad-chief.html?ESRC=topstories.RSS

U.S. embassy shuts down as Bangkok violence worsens. As clashes between protesters and the Thai military have escalated in a central area of Bangkok, Thailand, the U.S. embassy, located near the protest area, has shut down, at least until Monday. Since April 28, when it issued a travel alert, the State Department has advised U.S. citizens to avoid all non-essential travel to Thailand; some hotels in the capital city have urged guests to relocate. In addition, the United States government said on Saturday that it was offering a voluntary evacuation of non-essential personnel from Bangkok and advised against all travel to the city, as violence has continued to worsen in the Thai capital. Source: http://intransit.blogs.nytimes.com/2010/05/14/u-s-travelers-warned-as-bangkok-violence-escalates/?src=mv

Information Technology and Telecommunications

Facebook gives users' names to advertisers. Facebook has been giving advertisers data that they can use to discover users' names and locations, contrary to its privacy policy. The dominant social network tells users it will not share their details without consent, but according to the Wall Street Journal, it has handed over information that advertisers can use to look up individual profiles. MySpace had a similar loophole, it is reported. Both sites said they were making changes to stop the handover. Advertisers were getting reports whenever users clicked on their ads, as is typical across the Web. However, Facebook and MySpace's reports contained the URL of the user's profile page, which often included their real name or user name. Neither site had bothered to obscure the data, in breach of their own privacy policies. It is just the latest privacy failing by Facebook, which has

suffered heavy criticism this month. Major changes to its privacy settings are expected after it decided to publish users' private information, and Instant Message transcripts showed the CEO of Facebook calling those same users "dumb [expletive]s" for trusting him with their data. Source: http://www.theregister.co.uk/2010/05/21/facebook_ads/

Microsoft to give governments heads up on security vulnerabilities. Microsoft will share technical information on security vulnerabilities with some government organizations before it publicly releases security patches to help governments protect critical infrastructure. Government organizations that participate in both of two existing Microsoft programs designed to share security information with governments can get advance access to the vulnerability data through a new pilot program named the Defensive Information Sharing Program (DISP). Microsoft will start the pilot program this summer and begin the full program later this year, Microsoft's group manager for response communications said in an e-mail statement. The group manager said early access to that information would let the government organizations get an early start on risk assessment and mitigation. "This will allow members [of DISP] more time to prioritize creating and disseminating authoritative guidance for increasing network defensive posture actions," the group manager said. DISP is one of two pilot programs that a senior security program manager lead in the Microsoft Security Response Center, detailed in a blog post May 17. The senior security program manager also described another program to share with governments known as the Critical Infrastructure Partner Program. It provides insights on security policy such as approaches to help protect critical infrastructures. Source: http://fcw.com/articles/2010/05/19/web-microsoft-patch.aspx

Combat the malvertising threat. Malicious advertising, also referred to as "malvertising," is a relatively new attack vector for cyber criminals that is quickly on the rise. With malvertising, fake malicious ads are delivered (often via advertising networks) to well-known Web sites as a way to reach millions of users at once on Web sites they normally trust. Unlike typical spam or virus attacks, which rely on victims to click on a link in an e-mail or accidentally download an infected program, malvertising attacks are presented on popular Web sites and can download malicious code directly onto a user's computer when the victim views the compromised ad. By infiltrating an entire ad network, the criminal gains access to a broad number of syndicated Web sites that can spread malicious code even further. Millions of users have been infected by malvertising threats recently, as evidenced by the high-profile attacks on The New York Times, Gizmodo, TechCrunch, WhitePages.com and other sites. Based on data generated from Dasient's telemetry system, there are approximately 1.3-million malicious ads viewed per day. Traditionally, many publishers and ad networks only respond to a bad ad when a user complains about the problem, and one complaint could mean thousands have been infected already by a malvertisement. To deal with the threat, publishers and ad networks have had to manually investigate reports of bad ads, which takes time and resources. Because attacks are sporadic, it makes the source of the bad ad very hard to pin down. To-date, publishers and ad networks have not had an automated solution to address the malvertising problem. Source: http://www.net-security.org/secworld.php?id=9305

Microsoft warns of flaw affecting 64-bit Windows 7. A vulnerability in the Canonical Display Driver (cdd.dll) in 64-bit versions of Windows 7 and Windows Server 2008 R2, and Windows Server 2008 R2 for Itanium-based Systems, could allow remote code execution. "The Windows Canonical Display Driver does not properly parse information copied from user mode to kernel mode," states Microsoft in a security advisory published May 19. "In most scenarios, an attacker who successfully exploited

this vulnerability could cause the affected system to stop responding and automatically restart. It is also theoretically possible, but unlikely due to memory randomization, that an attacker who successfully exploited this vulnerability could run arbitrary code. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights." To take advantage of the vulnerability, the attackers would have to trick the user into viewing a "specially crafted image file with an affected application," likely hosted on a malicious Web site. To do that, it is likely that they would employ social engineering tactics such as sending an e-mail or an instant message containing the malicious link and purporting to be from a user's friend and with a link back to a curious/funny image, video, or test. Source: http://www.net-security.org/secworld.php?id=9313

Nanotech will be focus for future criminal hackers. Criminal hackers once rejoiced in manipulating the new digital phone systems in the 1960s and 1970s; then they moved on to using modems and hacking into mainframes in the 1970s and 1980s; then they exploited the new local area network technology and the burgeoning Internet in the 1980s. Malware writers moved from boot-sector viruses on floppy disks in the 1980s to file-infector viruses and then to macro viruses in the 1990s and vigorously exploited worms and Trojans for botnets in the recent decade. So what's next on the horizon? Recently a report in the "Random Samples" column by a contributor to SCIENCE magazine for Feb. 19, 2010 (Vol 327, p 927) told of the fuss in France "over the pros and cons of nanotechnology." Apparently in late January 2010, "the committee organizing the series of 17 debates threw in the towel, replacing the final two meetings with 'Internet workshops' and making the wrap-up event in Paris on 23 February by invitation only." The changes were the result of "heckling by antinanotech protesters in five cities." The question remains, however, of whether the agents of change are and will be taking the lessons of information security into account as they explore the possibilities of new technology. For example, the nanoparticles called polyamidoamine dendrimers (PAMAM) "cause lung damage by triggering a type of programmed cell deathâ_¦." The anti-nanotech organization NANOCEO (Nanotechnology Citizen Engagement Organization) has an enormous list of articles and scientific reports about the potential environmental risks of nanotechnology. Source: http://www.networkworld.com/newsletters/sec/2010/051710sec2.html

USB worm named biggest PC threat. A worm that is spreading via USB flash drives has been named the biggest security threat to PC users by McAfee. According to the security vendor's Threats Report: First Quarter 2010, an AutoRun-related infection was also the world's third biggest PC threat during the first three months of the year, while the rest of the top five biggest PC threats were made up of password-stealing Trojans. The report revealed that spam rates have remained steady. However, there has been an increase in diploma spam, or spam that offers forged qualifications, in China, South Korea and Vietnam. McAfee also said malware and spam in Thailand, Romania, the Philippines, India, Indonesia, Colombia, Chile, and Brazil had surged. The security vendor said this was due to the significant growth of Web use in these countries coupled with a lack of security awareness. "Our latest threat report verifies that trends in malware and spam continue to grow at our predicted rates," said a senior vice president and chief technology officer of Global Threat Intelligence for McAfee. "Previously emerging trends, such as AutoRun malware, are now at the forefront." Source: http://www.networkworld.com/news/2010/051810-usb-worm-named-biggest-pc.html?hpg1=bn

Koobface gang counter-poohpooh nemesis sec-pro Danchev. The gang behind the infamous Koobface worm has responded to a post by a security researcher on their activities and motives with an answer buried in the latest version of their malware. A noted security researcher posted a list of

"10 things you didn't know about the Koobface gang" in a blog post back in February. Koobface (an anagram of Facebook) is a worm that spreads on social networking sites. The worm, reckoned to be one of the most complex strains of malware yet seen, steals information from compromised hosts and promotes scareware sites, according to the researcher and anti-virus firms. Or not, according to the VXers behind the code. Late last week "Ali Baba" of the Koobface gang posted a point by point response as a message on Koobface-infected hosts, which served scareware disguised as bogus video codecs. Essentially the gang members attempt to paint themselves as elite coders in it for the lolz and not the loot. "What makes an impression is their attempts to distance themselves from major campaigns affecting high-profile U.S. based Web properties, fraudulent activities such as click fraud, and their attempt to legitimize their malicious activities by emphasizing the fact that they are not involved in crimeware campaigns, and have never stolen any credit card details," the researcher explained. Source: http://www.theregister.co.uk/2010/05/18/koobface_top_10_facts/

Web browsers leave 'fingerprints' as you surf. An overwhelming majority of Web browsers have unique signatures — creating identifiable "fingerprints" that could be used to track someone as they surf the Internet, according to research by the Electronic Frontier Foundation (EFF). The findings were the result of an experiment EFF conducted with volunteers who visited a Web site that anonymously logged the configuration and version information from each participant's operating system, browser, and browser plug-ins — information that Web sites routinely access each time one visits — and compared that information to a database of configurations collected from almost a million other visitors. EFF found that 84 percent of the configuration combinations were unique and identifiable, creating unique and identifiable browser "fingerprints." Browsers with Adobe Flash or Java plug-ins installed were 94 percent unique and trackable. EFF found that some browsers were less likely to contain unique configurations, including those that block JavaScript, and some browser plug-ins may be able to be configured to limit the information a browser shares with the Web sites one visits. But overall, it is very difficult to reconfigure a browser to make it less identifiable. The best solution for Web users may be to insist that new privacy protections be built into the browsers themselves. Source: http://www.net-security.org/secworld.php?id=9303

Cybersecurity summit pays little attention to control system's security. Despite threats of infrastructure attacks, scant attention was paid to control systems during a global security conference. As online attacks increase in severity and reach, targeting everyone from Google to the Pentagon, leading security experts and government officials met last week in Dallas at the EastWest Institute's first annual Cybersecurity Summit. The goal of the conference was to find common solutions to cybercrime and other online attacks, which respect no national boundaries. However, according to an InformationWeek's reporter, a major issue — for a meeting intended to find global solutions to information security challenges — is the fact that safeguarding control systems against attackers requires a different approach to securing PCs or networks. Windows-based security products will not help. "All the devices that sense things — temperature, pressure, flow, and things like that — are not Windows, those are proprietary, real-time or embedded, and there is no security there." Furthermore, seemingly rote IT activities, like installing antivirus on a control system, can actually create a denial of service. "Who needs hackers?" he said. Source: http://homelandsecuritynewswire.com/cybersecurity-summit-pays-little-attention-control-systems-security

BSA: $51 billion in unlicensed software exacerbates malware problem. The Business Software Alliance (BSA), which represents the commercial software industry and spearheads the effort to stop the spread of unlicensed applications, estimates in its Global Piracy Study 2010 that some $51.4 billion of unlicensed software was distributed in 2009. Aside from the cost to the software industry, the report said the high rate of piracy may be contributing to the spread of malware. The report makes reference to a previous study by International Data Corporation, which revealed that "one in four websites that offered pirated software or counterfeit activation keys attempted to install infectious computer code, like Trojan horses and key loggers, on test computers. Even more striking, 59 percent of the counterfeit software or key generators downloaded from peer-to-peer (P2P) sites contained malicious or unwanted code." The study also found the cost of recovery from a security incident resulting from pirated software on a PC can cost more than $1,000, often exceeding the cost of legitimate software. Source: http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=224800075

Google Street View accidentally collected user data via WiFi. Google May 14 said it will no longer collect WiFi data after discovering that its Street View cars unwittingly collected personal information from citizens' networks, a violation of privacy sure to inflame leaders of countries already wary of Google's data-collection practices. The search engine initially said in April that its Street View cars did not collect data that people share between WiFi networks and computers, although the cars did collect WiFi network names and router addresses. Google learned after conducting a data audit on behalf of the German government that this was incorrect. "It's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products," wrote a senior vice president of engineering and research. Payload data can include user e-mails, passwords and Web browsing activity, data the sanctity of which Internet companies such as Google, Yahoo and Microsoft swear to protect. Germany, the United States, Britain and France were among the countries where Google collected this data. Source: http://www.eweek.com/c/a/Search-Engines/Google-Street-View-Accidentally-Violates-User-Privacy-Via-WiFi-290159/

Remaining Facebook users warned about 'sexiest video'. Websense claimed that new malware is making its way across Facebook in messages that purport to contain 'the sexiest video ever'. When a user clicks on the 'video' they are taken to an application installation screen asking them to allow it to access their profile. Once approved, it claims they have to download an updated FLV Player to view the video and promptly sends an EXE to the user. It detected this as the Hotbar Adware that displays ads in one's browser based on browsing habits, etc. In addition, the Facebook application will post messages on a browsers' friends wall on the browser's behalf with the same 'sexiest video ever' message. The message has what appears to be a movie thumbnail of a woman on a bicycle wearing a short skirt, and the video's length is given as 3:17. Source: http://www.scmagazineuk.com/remaining-facebook-users-warned-about-sexiest-video/article/170322/

(Texas) **Security gaurd enters guilty plea for hacking employer's computers.** According to Computerworld, a former security guard has pleaded guilty to to two counts of transmitting malicious code for hacking into his employer's computers while working the night shift at a Dallas hospital. It wasn't hard to find the 25-year-old hacker, who goes by the name Ghost Exodus, as he posted videos of his misadventures to YouTube. Apparently, he is a member of a hacking group known as the

Electronik Tribulation Army and he installed the botnet code in an effort to take down a rival group's Web site. Each count carries a 10-year prison sentence. The man is scheduled to be sentenced September 16. Source: http://www.itbusinessedge.com/cm/community/news/sec/blog/security-gaurd-enters-guilty-plea-for-hacking-employers-computers/?cs=41199

National Monuments and Icons

(Pennsylvania) **Balloon containing flour prompts evacuation of Liberty Bell.** A park official said a white powder found in a balloon near the Liberty Bell in Philadelphia was flour. The balloon was found May 20 inside the building that houses the Liberty Bell. The Liberty Bell Center and part of a street next to it were evacuated as a precaution. A guard found the balloon inside the visitors entrance to the Liberty Bell Center, which is in downtown Philadelphia near office buildings, a federal courthouse and Independence Hall. Source: http://www.kwch.com/Global/story.asp?S=12516879

(Oklahoma) **Oklahoma tornado causes $13 million in damage to Lake Thunderbird.** Preliminary estimates released by officials with the state tourism department stated that the tornado that swept through central Oklahoma last week caused nearly $13 million in damage to public and private property on Lake Thunderbird. Members of the Tourism Commission May 19 approved an emergency declaration for the park that sustained major tornado damage. The declaration allows the department to issue contracts for cleanup, debris removal and reconstruction of structures damaged in the storm. The state will see a loss of approximately $1.9 million in damage to structures and lost revenue from the May 10 tornado. The twister damaged rest rooms at two campgrounds, camping areas and the Little River Marina on the north side of Lake Thunderbird. Storm damage also was reported at Lake Tenkiller, Lake Murray, Great Salt Plains, Boiling Springs and Sequoyah Bay state parks. Lake water quality wasn't affected. The marina at Lake Thunderbird had 250 boat slips and many of the boats remain scattered across the lake. Officials closed the lake for cleanup, but they expect to open it up again May 28 for the Memorial Day weekend. Source: http://www.newsok.com/oklahoma-tornado-causes-13-million-in-damage-to-lake-thunderbird/article/3462499?custom_click=pod_headline_usnational-news

Postal and Shipping

Man pleads guilty to anthrax threats. A transient pleaded guilty Monday to sending anthrax-hoax letters, threatening the President and failing to register as a sex offender. According to a plea agreement, the 62-year-old suspect admitted that he sent hoax mailings addressed to Social Security Administration offices that contained a white powdery substance and an index card with the words "you stole my money" and "die." As a result of the mailing to the New York Social Security office, 25 to 30 employees were evacuated, and four were quarantined, federal officials said. The suspect also admitted to making threats against the President. The letter to the President contained a white powder to simulate anthrax, prosecutors said. The suspect also admitted that, by virtue of a conviction in Texas, he was required to register as a sex offender in California and that he did not do so. He is scheduled to be sentenced August 2. The suspect faces a maximum statutory penalty of five years in prison and a $250,000 fine for sending hoax mailings and making threats to the president. For failing to register as a sex offender, he faces a maximum of 10 years in prison and a $250,000 fine. Source: http://www.kcra.com/mostpopular/23583695/detail.html

PUBLIC HEALTH

Vaccine shows promise against ebola virus. U.S. federal health researchers have developed an experimental vaccine that shows promise in protecting against the potentially deadly Ebola virus. Scientists with the National Institute of Infectious Diseases, the U.S. Army Medical Research Institute of Infectious Diseases and the Centers of Disease Control and Prevention said in a statement May 21, that the drug protected monkeys from two of the most lethal Ebola virus species, and a new species that was identified in 2007. No specific treatments or vaccines are available to control Ebola outbreaks, common on the continent of Africa. The researchers said the vaccine has two main components – a "prime" that is made up of a DNA vaccine containing a small piece of genetic material encoding surface proteins from the Zaire Ebola virus; and a "boost" that consists of a weakened cold virus that delivers the Zaire virus surface protein. The researchers recently found that it is protective in preventing the 2007 Bundibugyo virus. The report on the virus appears in the May 20 edition of the journal Public Library of Science Pathogens. Source: http://www.allheadlinenews.com/articles/7018763239

Poor security leaves VA systems open to attack, watchdog says. The Veterans Affairs Department (VA) runs unsecure Web application servers, uses weak or default passwords to protect its hardware and software, and does not comprehensively monitor connections between its systems and the Internet, according to an internal agency watchdog. These conditions leave department systems vulnerable to penetration or attack, said the VA Assistant Inspector in testimony before the House Veterans Affairs Committee Wednesday. The 2002 Federal Information Security Management Act requires federal agencies to develop, document and adhere to detailed information security programs. But the VA continues to have significant information security deficiencies. She said the IG office found several VA database systems used outdated software that could allow unauthorized users to access mission-critical data and alter databases. Most of VA's 153 hospitals do not segment access to their medical networks. As a result, IG investigators were able to penetrate the networks — including those hosting medical diagnostic and imaging systems — from remote locations. Source: http://www.nextgov.com/nextgov/ng_20100519_3450.php

U.S. stockpile receives new smallpox vaccine. The U.S. Strategic National Stockpile is now receiving shipments of a modified smallpox vaccine intended for people who have a compromised immune system and would not be able to safely receive the usual treatment, the Center for Infectious Disease Research and Policy reported May 17. The standard smallpox vaccine contains a live vaccinia virus that in a few cases can lead to serious health effects. The Imvamune vaccine is made from a less-potent version of the virus that is unable to duplicate itself and spread in humans. Though smallpox has been eradicated in nature, there are worries that the often lethal disease could be used in an act of biological terrorism. The U.S. government has procured sufficient quantities of the standard smallpox vaccine to safeguard all U.S. citizens should such an attack occur. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100518_3997.php

FDA widens Tylenol probe. The Food and Drug Administration (FDA) said Monday it is expanding its investigation of a Johnson & Johnson manufacturing division tied to the recent recall of children's drugs. On May 1, Johnson & Johnson's McNeil Consumer Healthcare unit recalled some 50 children's versions of non-prescription drugs, including Tylenol, Motrin and Benadryl. Then on May 6, the FDA issued a scathing 17-page inspection report of McNeil's Fort Washington, Pennsylvania, plant that

produced the drugs. Now the FDA is conducting a companywide investigation of McNeil's "manufacturing practices to determine whether similar problems exist throughout the company and what additional steps the agency must take to ensure that these problems do not recur," according to a statement posted Monday on the FDA Web site. In a statement e-mailed to CNNMoney Monday, McNeil said the company "is conducting a comprehensive quality assessment across its manufacturing operations and continues to cooperate with the FDA." Johnson & Johnson, which subsequently shut the Fort Washington facility, has declined to disclose what other products are manufactured at the plant. Source:
http://money.cnn.com/2010/05/17/news/companies/mcneil_fda_investigation/

P2P networks a treasure trove of leaked health care data, study finds. Nearly eight months after new rules were enacted requiring stronger protection of health care information, organizations are still leaking such data on file-sharing networks, a study by Dartmouth College's Tuck School of Business has found. In a research paper to be presented at an IEEE security symposium Tuesday, a Dartmouth College professor will describe how university researchers discovered thousands of documents containing sensitive patient information on popular peer-to-peer (P2P) networks. One of the more than 3,000 files discovered by the researchers was a spreadsheet containing insurance details, personally identifying information, physician names and diagnosis codes on more than 28,000 individuals. Another document contained similar data on more than 7,000 individuals. Many of the documents contained sensitive patient communications, treatment data, medical diagnoses and psychiatric evaluations. At least five files contained enough information to be classified as a major breach under current health-care breach notification rules. While some of the documents appear to have been leaked before the current administration's Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted, many appear to be fairly recent. A previous study by Dartmouth in 2008 also unearthed files containing health-care data floating on P2P networks, such as Limewire, eDonkey and BearShare. Among the documents found in that study was one containing 350 Megabytes of patient data for a group of anesthesiologists, and another with information on patients at an AIDS clinic in Chicago. Source:
http://www.computerworld.com/s/article/9176883/P2P_networks_a_treasure_trove_of_leaked_health_care_data_study_finds

(California) **Mumps outbreak may have entered Los Angeles County.** The Los Angeles Times reports that a mumps outbreak on the East Coast may have crossed the country to Los Angeles County. The newspaper reported May 16 that there have been nine cases of mumps reported in the county so far in 2010. That number is already two higher than what was reported in all of 2009. Of the nine cases reported so far, four may be related to a far larger outbreak in New York and New Jersey. There, the Times reports, more than 3,100 probable mumps cases have been reported, mostly in the Orthodox Jewish community. It is the largest outbreak in the U.S. in four years, according to the Los Angeles Times. The Los Angeles Times reports that the New York outbreak began in June 2009. An unvaccinated 11-year-old boy visited Britain, where mumps outbreaks are frequent. The paper states he then went to a summer camp and spread the disease. Source:
http://www.bioprepwatch.com/news/213073-mumps-outbreak-may-have-entered-los-angeles-county

Pharmaceutical companies provide EPA 100 drugs to help predict toxicity. The U.S. Environmental Protection Agency (EPA) will continue validating its ToxCast screening tool by screening more than

100 drugs provided by Pfizer, GlaxoSmithKline, Sanofi-Aventis, and Merck. These drugs never entered the marketplace because they demonstrated different types and levels of toxicity when the pharmaceutical companies conducted the early stage clinical trials required by the Food and Drug Administration as part of the drug development process. EPA researchers will quickly screen the drugs and then compare those results with the clinical trial results. Assessment of the similarities and differences in the results will improve EPA's ability to screen chemicals for toxicity. Because of the high cost and the long process of conducting chemical testing, only a small fraction of the thousands of available chemicals have been assessed for potential human health risk. EPA is using its ToxCast screening tool to help efficiently understand how chemicals may impact processes in the human body that could lead to adverse health effects. Currently, ToxCast includes 500 automated chemical screening tests that have assessed more than 300 environmental chemicals. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/90AAA37054ECBA04852577220054CBD

FDA: Glaxo, Merck vaccines OK despite pig virus. The Food and Drug Administration (FDA), in a statement, said it was safe for doctors to resume giving patients Glaxo's Rotarix and continue using Merck's Rotateq. The agency said there was no evidence that contamination caused any harm and the vaccines were important in preventing hospitalizations and death. Rotavirus can cause fatal diarrhea. Both vaccines target the virus, but pieces of DNA from porcine circovirus (PCV) have been found in both companies' products. The FDA's decision follows a May 7 recommendation by its advisory panel, which ruled that the risk to humans from the pig virus was theoretical at best. It called for continued use of the vaccines, saying their benefits outweighed any potential risk. Source: http://www.reuters.com/article/idUSTRE64D58I20100514

Transportation

FAA brass pushes NextGen. The Federal Aviation Administration's (FAA) biggest guns — current and past — turned out to urged the swift implementation and funding of NextGen, the satellite-based, air-traffic management system, at Aviation Week's "NextGen ahead" symposium in Washington, D.C. On Thursday, a former FAA administrator, now president of the Aerospace Industries Association, told the gathering, "It's time to reach consensus on accelerating NextGen." She said the question of which aviation users would benefit from the new system, which requires new equipment on aircraft, is misplaced since the benefits of reduced congestion and more efficient traffic movement with reduced fuel burn and emissions, benefit all. The current FAA administrator is to present evidence of the agency's commitment to ATC modernization in a presentation to the group this morning. Source: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=busav&id=news/awx/2010/05/20/awx_05_20_2010_p0-228456.xml

(New York) **Investigation into alleged TSA thefts at JFK airport.** They are the backbone of airport security. The TSA screeners who watch to make sure nothing dangerous is put into travel bags, but at John F. Kennedy International Airport (JFK), it's what's being taken out that has some passengers upset. Dozens of travelers have had valuables stolen while going through TSA screening checkpoints at JFK in just the past 8 months. Port Authority Police records show the thefts involve expensive bracelets worth thousands of dollars, high-end watches, iPhones, even prescription medications. In February, a woman's $3,000 watch disappeared from one of the bins as it went through X-ray at a JFK checkpoint. She strongly suspects a TSA agent took it, and she finds that deeply disturbing. "They're

stealing from us, this is a national security issue. What if somebody gives them $10,000 and says 'look the other way, let's put this bag through?' " said the woman. In the last three years, four TSA checkpoint screeners at JFK have been fired for theft while only one has been fired at Newark Airport, and 1 at LaGuardia Airport. Last July, two Kennedy Airport screeners got caught red-handed swiping a cell phone and laptop from luggage during a TSA integrity sting. The Port Authority said there have been 51 cases of theft at TSA check points at JFK in the last two years. Police sources said the number is probably much higher, especially since many times, the thefts are never reported. Source: http://abclocal.go.com/wabc/story?section=news/investigators&id=7447038

Water and Dams

Instant information about water conditions: Ask the river to text you a WaterAlert. Now one can receive instant, customized updates about water conditions by subscribing to WaterAlert, a new service from the U.S. Geological Survey (USGS). Whether one is watching for floods, interested in recreational activities or concerned about the quality of water in one's well, WaterAlert allows one to receive daily or hourly updates about current conditions in rivers, lakes and groundwater when they match conditions of concern. WaterAlert allows users to receive updates about river flows, groundwater levels, water temperatures, rainfall, and water quality at any of more than 9,500 sites where USGS collects real-time water information. This information is crucial for managing water resources, including during floods, droughts, and chemical spills. WaterAlert also allows kayakers, rafters and boaters to better understand when conditions are optimal and safe for recreational activities. WaterAlert users start at http://water.usgs.gov/wateralert and select a specific site. Users then select the preferred delivery method (email or text), whether they want hourly or daily notifications, which data parameter they are interested in, and the threshold for those parameters. Users can set the system to alert them when conditions are above a value, below a value, and between or outside of a range. Source: http://www.usgs.gov/newsroom/article.asp?ID=2464

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(In ND only); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**